UNITED STATES OF AMERICA	)	
	)	
v.	)	
	)	**STIPULATION OF**
Manning, Bradley E.	)	**EXPECTED TESTIMONY**
PFC, U.S. Army,	)	
HHC, U.S. Army Garrison,	)	**Mr. James McManus**
Joint Base Myer-Henderson Hall	)	
Fort Myer, Virginia 22211	)	**DATED: 7 June 2013**

It is hereby agreed by the Accused, Defense Counsel, and Trial Counsel, that if Mr. James McManus were present to testify during the merits and pre-sentencing phases of this court-martial, he would testify substantially as follows:

1. I currently work as an IT Architect at Brookhaven National Laboratory (BNL) in Upton, New York. In this capacity, I perform forensic imaging of the computers our Cyber Security Team confiscates and perform forensic analysis of those computers with Windows operating systems. I also control anti-virus for the approximately five-thousand computers connected to the BNL system, and run penetration testing on BNL servers to ensure they are secure. I work with Mr. Alex Withers. Mr. James Fung is my supervisor. I have held this position for two years. For the five preceding years, my job title was Senior Engineer; however, my responsibilities have remained the same. I have worked at BNL for thirty years, and have worked with the Cyber Security Group for ten of those years. For the past five years, I have attended at least one System Administration Network Security (SANS) course on network security and forensic examination per year. The courses also cover how to handle digital evidence.

2. I first became involved in this case after forensically imaging the hard drive of a desktop work station computer of a BNL employee identified as Mr. Jason Katz, which had been collected upon suspicion of having been used contrary to BNL policy. Based on BNL's report to federal law enforcement officials, investigators in the present case against PFC Manning became interested in the contents of the BNL desktop computer assigned to Mr. Katz, which I processed.

3. On 24 February 2010, I received a Dell Optiplex 960 desktop computer assigned to Mr. Katz from Mr. Alex Withers. After receiving the computer, I secured it in our evidence safe in our secure forensic evidence laboratory. The lab is accessible only to the six BNL Cyber Security team members, who must use secure key card to gain entry. A key and pass code are required to open the safe. It is only accessibly if either Mr. Fung or his associate, who also works in our Cyber Security Group, are present, as they are the only individuals with the required key. Only Cyber Security Group members have the required pass code.

4. On 25 February 2010, while in our secure forensic evidence laboratory, I removed the hard drive from the Dell Optiplex 960 BNL desktop computer collected from Jason Katz. I obtained a forensic image of this hard drive using the program FTK imager. I followed standard imaging procedures on which I have been trained and which I have used before.

5. A forensic image of an item of digital media is an exact copy of the data on the digital media. Digital forensic examiners image devices so that the originally-collected device can be

/ D 2

PROSECUTION EXHIBIT 75 **for identification**
PAGE OFFERED:____ PAGE ADMITTED:____
PAGE 1 **OF** 2 **PAGES**

forensically examined without risking contamination of the original data. This is standard practice by digital forensic examiners. The software forensic examiners use to image the digital evidence has built in procedures to verify that the item has been successfully duplicated. For example, the program will note the MD5 hash or Secure Hash Algorithm 1 (SHA1) hash value of an item of digital evidence before imaging (acquisition hash value) and after imaging the item (verification hash value). If the two hash values match, the item has been successfully duplicated bit-for-bit. The hash value is determined by mathematical algorithm and is displayed as a number/letter identifier unique to every item of electronically stored information. It is the equivalent of a digital fingerprint. When the hash value is generated, the entire hard drive will have a hash value, as well as each individual file on the hard drive. If there is any alteration to the hard drive or to any file on the hard drive, the acquisition and verification hash values will not match. The alteration can be as small as adding a single space into text document or saving the data to a different size device. In this case, I used FTK Imager forensic software to complete this imaging process. FTK Imager is similar to EnCase and is widely used by digital forensic examiners. I also used a write blocker when imaging this drive in order to ensure the originally collected evidence was not altered in any way. As I stated earlier, I have received training on FTK Imager and have used it in my other work. I encountered no errors while conducting the imaging of the evidence at issue in this case

6. I processed a BNL-owned Dell Optiplex 960 desktop computer hard drive with Linux operating system, serial number 9SZ3MBE3, bar code 138694. I made a forensic image of this drive for our lab's internal examination. In doing so, I identified the SHA1 hash value of the hard drive collected to be 60a5cd8caf580f7c1bba415f793550a7349af1bc. At no point during my handling of the evidence in question did I alter the computer, its hard drive, its other components, or its contents in any way. At no point did I observe anyone alter the computer, its hard drive, its other components, or its contents in any way. I have no reason to believe the evidence was damaged or contaminated in any way.

	Thomas F. Hurley	
ASHDEN FEIN MAJ, JA Trial Counsel	THOMAS F. HURLEY MAJ, JA Defense Counsel	BRADLEY E. MANNING PFC, USA Accused